IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

Authenticom, Inc., *Plaintiff*, vs. CDK Global, LLC; and The Reynolds and Reynolds Company, *Defendants*.	Case No. 17-cv-318 Hon. James D. Peterson

DEFENDANT CDK GLOBAL, LLC'S MEMORANDUM
IN SUPPORT OF ITS MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

Statutes, Rules and Regulations

Other Authorities

INTRODUCTION

Authenticom's theory of this case is predicated on several fundamental legal errors and factual self-contradictions that doom its complaint to dismissal. In saying this, we are mindful that the Court held in its opinion on the motion for a preliminary injunction that there is a "moderate chance" Authenticom will succeed on its Section 1 antitrust claims. *See* Dkt. 172, at 1, 11-16. But in coming to that conclusion, the Court did not address the principal legal deficiencies in the complaint. Those deficiencies—taking account of no more than the complaint's allegations and incorporated documents—require a dismissal of the lawsuit, notwithstanding the order granting a preliminary injunction.

First, the agreements between CDK and Reynolds on which Authenticom bases its complaint do not say what Authenticom alleges. As the Court expressly acknowledged in its preliminary injunction opinion (*id.* at 6-7), the CDK-Reynolds data access agreement neither required CDK to refrain from offering integration services to Reynolds dealers nor obligated Reynolds (which had never engaged in hostile integration) to refrain from offering integration services to CDK dealers. Nor does the agreement require either firm to block Authenticom—something that each defendant admittedly could accomplish unilaterally. *See, e.g.*, Compl. ¶ 6. [redacted]. The RCI and 3PA Agreements do not help Plaintiff's claims either; [redacted].

Second, and in any event, neither CDK nor Reynolds had anything to gain from an unlawful conspiracy. In Authenticom's own telling (Compl. ¶ 6), Reynolds began unilaterally blocking hostile, unauthorized access to its systems at least as early as 2007. It needed no agreement with CDK to take that action. For its part, CDK allegedly began blocking hostile access in 2015. *Id.* ¶ 98.

It, too, needed no agreement with Reynolds to begin blocking Authenticom and other hostile integrators. What, then, did either defendant have to gain from conspiring with the other? The answer is simply *nothing*. And if a defendant "had no rational economic motive to conspire, and if their conduct is consistent with other, equally plausible explanations, the conduct does not give rise to an inference of conspiracy." *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 596-597 (1986). That is the case here.

Third, the antitrust laws do not protect business models predicated on inducing violations of valid service contracts and federal and state laws, as Authenticom's business model is. All along, CDK's service agreements with dealers have prohibited dealers from granting access to CDK's systems to third parties like Authenticom. Compl. ¶ 151. The Court did not hold in its opinion on the preliminary injunction that CDK's dealer service agreements are unlawful; indeed, Authenticom's own service agreements contain a virtually identical provision. Yet Authenticom proudly touts that it has surreptitiously circumvented CDK's efforts to block unauthorized access to CDK's systems. Compl. ¶ 195. And it does not deny that the nub of its service is to incite dealers to violate the clear terms of their service agreements with CDK. As Reynolds explains at greater length in its separate dismissal motion, moreover, Authenticom has no answer to our demonstration (Dkt. 105, at 47-49) that its unauthorized access to defendants' systems violates the federal Computer Fraud and Abuse Act and Wisconsin Computer Crimes Act. This is not conduct that the antitrust laws protect or that this Court should countenance.

Finally, none of the complaint's other theories holds up to scrutiny. With respect to tying, the complaint does not allege that CDK required dealers to purchase a secondary service from CDK against their wishes—not the least because dealers all along have been aware that unauthorized third-party access by "integrators" like Authenticom violates their service agreements, and because dealers do not purchase "integration" services in any event. What is more, there are ample and obvious procompetitive justifications for CDK's decision to begin more aggressively enforcing its

right to block unauthorized access to its systems. CDK "had the right to [design and] redesign [its] products to make them more attractive to buyers" through "improved performance"; the antitrust laws do not impose a duty to limit "product development so as to facilitate sales of [Authenticom's] products." *Allied Orthopedic Appliances Inc. v. Tyco Health Care Grp. LP*, 592 F.3d 991, 999 (9th Cir. 2010) (quoting *Cal. Comput. Prods., Inc. v. IBM*, 613 F.2d 727, 744 (9th Cir. 1979)). Authenticom's only response is a naked allegation that CDK's explanations are pretextual—but mere labels are not enough. For these and all of the reasons given below, the complaint should be dismissed.[1]

BACKGROUND[2]

A. The DMS market

Automobile dealerships generate large volumes of data in the course of their operations, including inventory, customer, sales, financing, and insurance information. Compl. ¶ 2. DMSs are the enterprise software platforms that dealerships use to collect, manage, and manipulate this data. *Id.* ¶ 29.

The market for DMS services in the United States comprises a number of firms of various sizes. Reynolds and CDK are two of the largest firms serving new vehicle franchised dealers. Compl. ¶ 33. CDK was formerly a subsidiary of Automatic Data Processing, Inc. (ADP) until it was spun off in 2014. *Id.* ¶ 20. Authenticom alleges that, by number of franchised stores served, CDK

[1] We appreciate the Court's considerable efforts to date in holding an evidentiary hearing and accepting lengthy submissions related to Authenticom's request for preliminary injunctive relief. The purpose of this motion is to set forth why, as a matter of law, Authenticom has failed to meet the stringent standards necessary to plead a Section 1 claim, whatever the merits of its irreparable injury claim. The written agreements between Reynolds and CDK do not satisfy Authenticom's burden and, as discussed below, neither do the bare allegations that representatives of Reynolds and CDK admitted to a conspiracy. In light of the substantial discovery and related burdens that antitrust litigation may place on parties, and not wishing to waive or otherwise be thought to acknowledge that there is a legal basis for Authenticom's antitrust claims, we respectfully submit this motion to the Court.

[2] We describe here the allegations in the complaint, which are assumed true for purposes of this motion. *Firestone Fin. Corp. v. Meyer*, 796 F.3d 822, 826 (7th Cir. 2015). CDK does not, however, concede the truth of the facts alleged.

has an approximate 45% share of the U.S. market for DMS services. *Id.* ¶ 33. Reynolds, which formerly was publicly traded but was taken private in 2006 (*id.* ¶ 21), purportedly has an approximate 30% share of the market. *Id.* ¶ 33. There are also an "array" of smaller providers in the market, providing service to approximately 30% of the new vehicle franchised dealers in the U.S. *Id.* ¶ 35. DMS firms fiercely compete to attract dealers' business from one another. *See, e.g.*, *id.* ¶ 42 (describing competition between Reynolds and CDK for Hendrick Automotive Group, the sixth largest dealership group in the country).

B. CDK's restrictions on DMS access

Cybersecurity and system performance are essential to the proper functioning of CDK's DMS platform. In part to ensure that CDK is able to maintain the security and stability of its systems, the terms of its DMS service contracts with dealers have long expressly prohibited dealers from granting any unauthorized third party access to the DMS, including by creating login credentials for third parties. *See* Compl. ¶ 151 [redacted]

C. Authenticom's unauthorized access

Many dealers contract with one or more third-party software vendors, who offer software applications that perform sales and other operational functions for dealerships. Compl. ¶ 48. Hundreds of different vendors offer a wide variety of services to dealerships in this way. For example, some vendors help dealers schedule service appointments. *Id.* Others provide vehicle registration services at the time of sale, manage customer outreach, or assist with other services. *Id.* *See generally, e.g.*, perma.cc/EB4R-H7R7 (website listing scores of highly-rated DMS applications).

To operate most effectively, vendors may access data collected by dealers. A service-scheduling vendor, for example, would benefit from access to the dealer's customer and vehicle maintenance records. A vendor like CARFAX would need access to a dealer's inventory and the VINs associated with each vehicle. Many vendors require only the ability to "pull" data, but others

also require the ability to "push" or "write-back" altered or edited data into the DMS so that it can populate the DMS's various workflows, as when a vendor amends individual customer records. Compl. ¶ 50.

Dealers do not ordinarily provide direct access to the defendants' proprietary DMSs to these third-party vendors. Some vendors wishing to access a system contract with independent data "integrators," who—acting as middlemen between the DMS platforms and vendors—obtain data from the DMS and provide it to vendors through the "integrator's" own software interface. Compl. ¶ 54. Dealers have typically facilitated data "integrator" access to the DMS by either sharing existing login credentials or creating new ones for the "integrators." These "integrators" then use those credentials to emulate dealership employees, pulling data from the DMS in an automated fashion, screen-scraping it, providing the data to vendors, and, in some instances, pushing altered or amended data into the DMS. *Id.* ¶ 77. When used in connection with CDK's system, this process has necessarily required the dealers to violate the terms of their DMS contracts with CDK, since those contracts forbid dealers from giving third parties access to the DMS. Compl. ¶ 151. For this reason, access by third-party "integrators" is known as "hostile" access.

Plaintiff Authenticom is a data "integrator" that contracts with a number of vendors to pull data from, and, in some instances, push data to, various DMS platforms. Its core product is DealerVault, a "unified user interface" that purportedly allows dealers to control what data is sent to Authenticom's vendor customers. Compl. ¶ 78. Authenticom does not provide any specifics regarding its cybersecurity measures, policies, or practices, nor does it offer the results of any cybersecurity audits by an independent organization.

D. CDK's SecurityFirst initiative and 3PA program

Beginning in 2015, CDK revamped its approach to transporting data to and from its DMS by enhancing its Third-Party Access (3PA) program. Compl. ¶¶ 98-99. This change was made as part of CDK's SecurityFirst initiative, which was intended to improve the security of the CDK DMS. *Id.*

¶ 99. Under the new 3PA program, vendors could no longer obtain data from hostile third parties like Authenticom; instead, they were required to obtain data through the 3PA interface. *Id.* ¶ 98.

E. Reynolds provides an orderly wind-down of CDK subsidiaries' hostile access

By 2013, as technology improved, Reynolds's ability to disrupt automated hostile "integrators" attempting to sell services to other third parties was virtually complete. Compl. ¶ 189 ("Reynolds's [blocking] actions resulted in an almost complete collapse of Authenticom's integration business for dealer data for dealers using the Reynolds DMS."). At the time, ADP (from which CDK was later spun off) owned two subsidiary companies—Digital Motorworks (DMI) and IntegraLink—that operated as, among other things, data "integrators." *Id.* ¶ 89. Both DMI and IntegraLink engaged in hostile access to Reynolds's systems. *Id.* ¶ 90. Reynolds—as it had with all other hostile integrators that attempted automated access to its system—demanded that DMI and IntegraLink cease their activities. Ultimately, CDK decided, as a business matter, to cease hostile integration activities entirely and thus agreed that DMI and IntegraLink would stop attempting to hostilely integrate into Reynolds's DMS. *Id.* ¶ 132.

Not wanting to leave their shared customers high-and-dry, Reynolds and CDK negotiated an agreement for a voluntary wind-down of DMI and IntegraLink's hostile access to Reynolds's system. The agreement, entered into in February 2015, was a [redacted] *See* Ex. 1. It bears emphasis that the document that Authenticom has produced and quoted from in its complaint is not the agreement between Reynolds and CDK; it is, instead, a draft Wind Down Access Agreement that Reynolds offered to *Authenticom*, in conjunction with Reynolds's demand that *Authenticom* cease unauthorized access of Reynolds's systems. *See* PI Mot. Ex. 46, ECF No. 65-21 ("WHEREAS, Authenticom and Reynolds wish to settle their disputes…").[3]

[3] Defendants have attached the actual agreements to this motion as Exhibits 1-3. The court can consider them in ruling on the motion, because Authenticom clearly meant, in its complaint, to refer to defendants' actual agreements (despite never having seen them), and when "a plaintiff mentions a document in his complaint, the defendant may then submit the document to the court without

Authenticom alleges that the [redacted] Compl. ¶ 134. But this statement appears nowhere in the actual 2015 agreement. CDK and Reynolds specifically did not come to an agreement regarding either company's policies with respect to accessing each other's DMS. [redacted] l. *See* Ex. 1. Indeed, [redacted] t:

[redacted]

In other words, all CDK and Reynolds were prohibited from doing [redacted]. No more, no less. The contract does not obligate CDK or Reynolds to block hostile integrators or close their respective DMSs. This contract did not impinge on DMI and IntegraLink's ability to integrate (hostilely or otherwise) [redacted]. Similarly, Authenticom (or any other third party provider) could continue to attempt to hostilely integrate (including into CDK and Reynolds' systems) on their own [redacted].

converting defendant's 12(b)(6) motion to a motion for summary judgment." *See, e.g.*, *Brownmark Films, LLC v. Comedy Partners*, 682 F.3d 687, 690 (7th Cir. 2012).

As part of the 2015 agreement, the parties signed two additional contracts.[4] First, [redacted] *See* Ex. 2. [redacted].

Second, [redacted]. *See* Ex. 3. [redacted].

Nothing in the [redacted] agreements obligates CDK or Reynolds to block hostile integrators or close their DMS systems. [redacted] Again, Authenticom and other third parties were free to try to hostilely integrate with either CDK's or Reynolds's systems. Both CDK and Reynolds remained free to compete with each other as DMS providers and as application providers, and both remained free to do business (or refrain from doing business) with Authenticom as each unilaterally saw fit.

ARGUMENT

In determining whether a complaint has failed to state a claim under Rule 12(b)(6), a court accepts as true "all well-pleaded facts" and draws all inferences in favor of the plaintiff. *Bielanski v. Cty. of Kane*, 550 F.3d 632, 633 (7th Cir. 2008). The complaint must, however, "include 'enough

[4] Because they were part of a single transaction with, and incorporated by reference into, the [redacted], these agreements are also properly considered on this motion to dismiss. *See supra* note 3.

facts to state a claim to relief that is plausible on its face.'" *Khorrami v. Rolince*, 539 F.3d 782, 788 (7th Cir. 2008) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007)). Put differently, the factual allegations in the complaint must "plausibly suggest that the plaintiff has a right to relief, raising that possibility above a 'speculative level'; if they do not, the plaintiff pleads itself out of court." *EEOC v. Concentra Health Servs., Inc.*, 496 F.3d 773, 776 (7th Cir. 2007) (quoting *Twombly*, 550 U.S. at 545).

The allegations in the complaint tell a straightforward and consistent story: Plaintiff Authenticom is a for-profit third-party data "integrator" that accesses defendants' systems, without authorization and without paying anything to defendants, in order to extract data and provide it to vendors. Defendants have each implemented programs—at different times—requiring vendors to access dealers' data through secure interfaces built into the DMS itself. In response, Authenticom has brought this suit under the Sherman Act, making the remarkable assertions that the antitrust laws (1) *forbid* defendants from enforcing the terms of their contracts with dealers (which forbid access by third parties like Authenticom) and (2) *require* defendants to grant Authenticom unfettered access to their proprietary systems, on Authenticom's terms, so that Authenticom's obsolete business model can survive.

Both assertions are wrong: courts have routinely held that absent exceptional circumstances not present here, a firm has no duty under antitrust law to deal with would-be rivals and provide them assistance. In an effort to stave off the unavoidable, Authenticom alleges a horizontal conspiracy and market-division scheme that is by turns completely implausible and belied by the terms of the actual written agreement between defendants (an agreement that Authenticom had not seen when it filed its complaint). None of Authenticom's remaining claims—tying, group boycott, exclusive dealing, and tortious interference with contract—fits the facts alleged. The bottom line is that Reynolds and CDK have compelling procompetitive reasons to design their respective systems to prevent hostile third-party data "integrators" like Authenticom from accessing them. The antitrust

laws *encourage* this kind of innovation, rather than condemning it. For this reason and all of those given below, Authenticom has failed to state any plausible claim for relief under the Sherman Act. The complaint should accordingly be dismissed.

I. AUTHENTICOM HAS FAILED TO STATE A CLAIM UNDER SECTION 1

A. Authenticom's horizontal conspiracy claims are implausible

1. The allegations of a market-division agreement are implausible

The centerpiece of Authenticom's case is its allegation that Reynolds and CDK entered into a "written agreement" that they "would no longer compete in the Dealer Data Integration Market." Compl. ¶ 132. It is implausible on its face that defendants—sophisticated business entities represented by experienced in-house and outside counsel—would commit a *per se* violation of the Sherman Act by reducing it to a lengthy written agreement. But setting that aside, Authenticom is simply wrong about what that agreement says.

The actual 2015 agreement between Reynolds and CDK comprises three separate contracts: (1) a [redacted] between Reynolds and CDK related to winding down DMI's and IntegraLink's unauthorized access to the Reynolds systems; (2) a [redacted] providing a [redacted]; and (3) a [redacted] governing [redacted]. *See* Exs. 1-3. There is no agreement by either party with respect to each other's DMS system access policies or anything else about their policies regarding interactions with data "integrators." *See id.* The supposed "market division" agreement is, in actuality, an agreement to facilitate CDK's decision to wind down the unauthorized access of its subsidiaries to Reynolds's systems.

Authenticom alleges that the agreement divided "a substantial portion of the dealer data integration market" (Compl. ¶ 257), in that CDK "agreed that it would no longer compete in providing access to dealer data on the Reynolds DMS" (*id.* ¶ 132). Not so. Reynolds has

aggressively enforced its service contracts to prevent unauthorized access to its DMS since at least 2007 (*see* Compl. ¶ 6); it needed no agreement with CDK to continue doing so. The same goes for CDK, which independently introduced SecurityFirst and began enforcing its own bans on third-party access in 2015. *Id.* ¶ 98. Neither defendant needed to *agree* with the other to enforce their prohibitions on unauthorized system access to their respective DMSs. And if defendants "had no rational economic motive to conspire, and if their conduct is consistent with other, equally plausible explanations, the conduct does not give rise to an inference of conspiracy." *Matsushita*, 475 U.S. at 596-97. That is the case here: Neither CDK nor Reynolds had any economic motive to conspire because no market division agreement could have improved either defendants' market position.

To be sure, the Court held in its opinion on the motion for a preliminary injunction that there was evidence that Authenticom's CEO had been told by defendants' employees that "they had agreed to drive Authenticom from the market." Dkt. 172, at 12. But even if that were the case, that is not enough to survive a Rule 12(b)(6) motion in a Section 1 antitrust case; again, to plead a plausible conspiracy, Authenicom must allege a "rational economic motive" for such an agreement. *Matsushita*, 475 U.S. at 596. That motive is wholly absent from the complaint.

Nor does the 2015 agreement amount to a market-division scheme as a logical matter. To the extent that CDK was agreeing that DMI and IntegraLink would stop hostilely accessing Reynolds's systems (and it was not), this would have *helped* Authenticom by eliminating two of Authenticom's key competitors for data extraction services. Besides that, Reynolds has never provided hostile integration on CDK's (or any other DMS provider's) system, so any agreement on its part plainly does not fit with a market division theory, either. *Cf. Cal. ex rel. Harris v. Safeway, Inc.*, 651 F.3d 1118, 1137 (9th Cir. 2011) (illegal "market-allocation agreements" are "among competitors at the same market level").

2. CDK did not agree to a "group boycott"

Authenticom also alleges that defendants engaged in a "group boycott" in violation of Section 1 of the Sherman Act. In Authenticom's telling, defendants sought to "block all other third-party data integrators (such as Authenticom) from accessing data of dealers" on their respective DMSs. Compl. ¶ 245. This theory, too, is conceptually flawed.

A group boycott occurs when "firms with market power boycott suppliers or customers in order to discourage them from doing business with a competitor." *FTC v. Ind. Fed'n of Dentists*, 476 U.S. 447, 458 (1986). The theory is one, therefore, of a "concerted refusal to deal." Phillip E. Areeda & Herbert Hovenkamp, *Antitrust Law: An Analysis of Antitrust Principles and Their Application* ¶ 2202 (June 2017) ("Areeda & Hovenkamp"). But there is no refusal to deal here; defendants do not "deal" with Authenticom, which gets login credentials from dealers (not Reynolds or CDK) and has a service relationship with vendors (again, not Reynolds or CDK).

The Court held otherwise in its preliminary-injunction opinion (Dkt. 172, at 13), but that legal analysis was incomplete. The Court held, in particular, that "defendants agreed that *in their capacity as app providers*, their sole access to one another's DMSs would be through the in-house interfaces." *Id.* (emphasis added). "In other words," according to the Court, "by signing up for 3PA or RCI, defendants agreed not to use third-party integrators to access the CDK DMS or the Reynolds DMS, respectively" for purposes of running their *own* DMS apps. *Id.*[5] But this is not a theory alleged in the complaint; indeed, the complaint does not even allege that defendants control or operate any apps; and, in actual fact, they are but two of many app providers in the marketplace. As the Court recognized with respect to defendants' alleged vertical agreements (Dkt. 172, at 15), it is fundamental that "even though a contract is found to be an exclusive-dealing arrangement, it does

[5] Respectfully, that is not an entirely accurate description of what the relevant contracts say. As described in detail above (at 8), [redacted]. *See generally* Exs. 2 and 3.

not violate the [antitrust laws] unless the court believes it probable that performance of the contract will foreclose competition in a substantial share of the line of commerce affected." *Tampa Elec. Co. v. Nashville Coal Co.*, 365 U.S. 320, 327 (1961) (Clayton Act case). There is not an inkling of a suggestion in the complaint that the 3PA and RCI agreements foreclosed a substantial share of the market for data integration services; nor, in light of the facts known to the Court, could there ever be.

Authenticom's "group boycott" theory, like its also falters logically for the same reasons as does its "market division" theory. In order to prove that defendants entered into an unlawful horizontal conspiracy, Authenticom must show that defendants engaged in parallel conduct, along with facts that "tend[s] to exclude the possibility of independent action." *Twombly*, 550 U.S. at 554. It has failed to show either. There is no allegation of "parallel" conduct: on the contrary, it is undisputed that Reynolds unilaterally forbade access to its DMS by hostile integrators years before CDK's SecurityFirst initiative. *See, e.g.*, *In re Musical Instruments & Equip. Antitrust Litig.*, 798 F.3d 1186, 1196 (9th Cir. 2015) (noting that according to the complaint, defendants "adopted the policies [at issue] over a period of several years, not simultaneously. Allegations of such slow adoption of similar policies does not raise the specter of collusion"). And second, Authenticom has not plausibly alleged facts that tend to exclude the possibility that defendants acted independently. Once again, there was nothing to gain from any supposed collusion, since both had the ability to shut down unauthorized third-party access to their systems unilaterally. *See Matsushita*, 475 U.S. at 596-97. And as the complaint suggests, there is an obvious innocent explanation for the agreements: Neither wanted to be sued by the other for tortious interference, as Reynolds is alleged to have done in prior cases. Compl. ¶¶ 107, 180.

In an attempt to paper over the implausibility of its conspiracy theory, Authenticom alleges that representatives of defendants confessed a conspiracy to Authenticom. But those allegations are nonsensical. For example, Authenticom alleges that Robert Schaefer from Reynolds told Authenticom's founder, Steve Cottrell, in May 2015 that CDK and Reynolds had an agreement "to support

each other's 3PA and RCI programs and therefore block competitors like Authenticom from pulling dealer data." Compl. ¶ 181. To begin with, as we demonstrated above, the 3PA and RCI agreements between CDK and Reynolds in no way "block" Authenticom from anything. There is no reference at all to Authenticom in either agreement. Moreover, such a statement would have made no sense—as Authenticom's own allegations acknowledge, Reynolds had made the decision many years earlier to enforce its prohibitions on unauthorized third-party data access. *See*, *e.g.*, *id.* ¶ 6. Thus, any statement that defendants would be "support[ing] each other's" data interface programs, if such statements were made, would have been consistent with the lawful Data Exchange Agreement and its supporting agreements.

Authenticom also alleges that Dan McCray, a CDK employee, told Cottrell that "Reynolds and CDK had agreed to 'lock [Authenticom] and the other third parties out.'" Compl. ¶ 180. But this alleged statement, without more, does not tend to exclude independent conduct. Moreover, as far as the complaint indicates, Cottrell did not take any of the steps one would expect of the founder of a company at which a life-threatening conspiracy was aimed: he did not object to CDK about the alleged statement, did not reveal the alleged statement to the public, and took no legal action until this lawsuit was filed over a year later. These omissions make implausible Authenticom's allegation that the conversation "confirmed the existence of [an] illegal agreement." *Id.*

B. CDK's agreements with its dealers are not "tying" agreements

Authenticom's next Section 1 theory—that defendants' agreements with dealers are "tying" agreements—fails as a matter of law and of logic. Tying is a specialized concept in antitrust law with a narrow definition, and Authenticom's attempt to shoehorn the facts of this case into that definition is plainly meritless.

A tying arrangement is "defined as an agreement by a party to sell one product but only on the condition that the buyer also purchases a different (or tied) product, or at least agrees that he will not purchase that product from any other supplier." *N. Pac. Ry. Co. v. United States*, 356 U.S. 1, 5-6

(1958); *see also, e.g.*, *A.O. Smith Corp. v. Lewis, Overbeck & Furman*, 979 F.2d 546, 547 (7th Cir. 1992) ("Tying arrangements involve an agreement to sell one product (the tying product) only on the condition that the purchaser buy a second product (the tied product)."). Thus, the essence of a tie is not merely that two products are related or designed to work together in certain ways. Rather, the seller must condition its sale of one product on its selling a second product *to the same buyer*: "[T]he essential characteristic of an invalid tying arrangement lies in the seller's exploitation of its control over the tying product to force *the buyer* into the purchase of a tied product that *the buyer* either did not want at all, or might have preferred to purchase elsewhere on different terms." *Jefferson Par. Hosp. Dist. No. 2 v. Hyde*, 466 U.S. 2, 12 (1984) (emphases added); *accord* Areeda & Hovenkamp ¶ 1752b ("There is no tie for any antitrust purpose unless the defendant improperly imposes conditions that explicitly or practically require buyers to take the second product if they want the first one.").

Authenticom alleges that CDK's dealer agreements meet this description because, "as a condition of dealers using [d]efendants' DMS services, [they] also require dealers to use [d]efendants' own integration services." Compl. ¶ 264. That description is plainly mistaken, because dealers do not themselves buy or "use" hostile data extraction services. Where hostile data "integrators" are involved in pulling data, it is *vendors* who engage them. *See id.* ¶ 59 (dealers "do not pay integrators to pull their data. Instead, vendors pay integrators for their data services."); *id.* ¶ 60 ("Vendors enter into contracts with data integrators to pull the data."). Moreover, dealers are not required to authorize any integration services, if they opt not to use any vendor applications. Dealers, therefore, are not required to take any separate product as a condition for obtaining CDK's DMS services—and accordingly are not subject to any unlawful tie.

Authenticom may attempt to sidestep this difficulty by arguing that vendors can only access data from dealers through a hostile integrator if the dealer has authorized that integrator and given it login credentials. But the role dealers might play in transactions between vendors and data

integrators is beside the point. Tying requires that the *buyer* of the two tied products be the same, because the essence of a tying violation is a seller's use of economic leverage over a buyer to induce *that buyer* to make additional purchases it prefers not to make. *See Jefferson Par. Hosp.*, 466 U.S. at 12. Authenticom's obfuscations notwithstanding, dealers do not buy data extraction services, which precludes any claim of a tie.

But even if that were not so, Authenticom's assertion (Compl. ¶ 268) that CDK's protection of its system is unlawful *per se* would fail. Although judicial decisions once spoke of tying arrangements as per se illegal, the law has since "backed away from flat condemnation of tying arrangements because they are not always abusive, and when they are not, they are a legitimate method of competition." *Batson v. Live Nation Entm't, Inc.*, 746 F.3d 827, 831 (7th Cir. 2014). Indeed, the leading commentators note that "the per se rule against tying is 'per se' in only one respect—namely, dispensing with proof of anticompetitive effects . . . . It expressly requires proof of power in the market for the tying product, as well as allowing defenses." Areeda & Hovenkamp ¶ 1760e3 (footnotes omitted). Even if defendants' service agreements with dealers did impose a tie (again, they do not), those agreements would have to be upheld under the Rule of Reason, in light of their procompetitive justifications. *See infra* at 18-20.

C. CDK has not engaged in exclusive dealing

Authenticom's final Section 1 theory is that defendants' agreements with dealers and vendors are "exclusive deals" that foreclose competition. This theory, too, is a conceptual mismatch for the facts that Authenticom alleges.

An exclusive dealing agreement is one in which a buyer and seller agree to deal with each other exclusively with respect to a particular good or service, foreclosing a portion of the market for other sellers of the good or service. *See* Areeda & Hovenkamp ¶ 1800a (explaining that an exclusive-dealing agreement "forbids the buyer from purchasing the contracted good from any other seller" or "requires the buyer to take all of its needs in the contracted good from that [seller]"). For

example, a manufacturer may require a dealer not to sell the goods of rival manufacturers. Or a seller may forbid a buyer from buying products from any other supplier.

CDK's contracts with its dealers do not fit either description. To begin with, Authenticom's argument is clearly inapt with respect to CDK's service contracts with dealers because *dealers* are not the purchasers of Authenticom's (or other data extraction) services. Nor can CDK's agreements with vendors who wish to access data housed on CDK's DMS platforms be exclusive dealing agreements. As Authenticom sees it, the agreements require vendors exclusively to "us[e] CDK or Reynolds for data integration services." Compl. ¶ 157. But 3PA is not a competing data integrator; it is a managed interface that is integral to CDK's DMS itself and allows vendors to obtain data directly from CDK rather than engaging third parties. *See id.* ¶ 98 (3PA allows vendors to "obtain data directly from CDK"); *see also id.* ¶ 47 (explaining that data integrators are "companies that provide service to dealers and application providers by pulling dealer data from the DMS, formatting and aggregating it, and then providing it to application providers").

What is more—as we explained above (at 5)—Authenticom's business model is predicated on inducing *dealers* to breach the express terms of their service agreements with CDK, which forbid unauthorized third-party access to CDK's systems. If Authenticom was content to induce breaches of those terms by dealers without claiming an antitrust violation, what should stop it from inducing similar breaches of CDK's agreements with vendors, which merely include mirror-image terms forbidding vendors from obtaining data by unauthorized means? At the least, if CDK's contracts with vendors are violations of the antitrust laws, so too must be its flipside contracts with dealers. Yet Authenticom does not seriously argue—and this Court did not hold—that CDK's contract terms with dealers forbidding unauthorized access are violations of the antitrust laws, not the least because such contract terms are commonplace throughout the national economy. Indeed, Authenticom includes nearly an identical term in its *own* service contracts with dealers. Authenticom gives no explanation whatever for this fundamental contradiction in its theory of the case.

D. In any event, CDK's conduct with respect to third party access easily survives the Rule of Reason

Even if everything we had said so far were wrong, CDK's conduct would be a basis for antitrust liability only if it could not be explained by "valid business reasons." *Eastman Kodak Co. v. Image Tech. Servs., Inc.*, 504 U.S. 451, 483 (1992) (quoting *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585, 605 (1985)); *accord, e.g.*, *Viamedia, Inc. v. Comcast Corp.*, 2017 WL 698681, at *4 (N.D. Ill. Feb. 22, 2017) ("[P]laintiffs seeking to establish an unlawful refusal to deal must show that the defendant's actions serve no rational procompetitive purpose."). Here, as Authenticom acknowledges, CDK's conduct rested on a clear and important business justification: the need to protect its system and the data on that system from cybersecurity threats. Compl. ¶ 235. That justification exonerates CDK, no matter what label Authenticom places on its conduct.

Authenticom's complaint does not allege that cybersecurity is not a concern for DMS providers (or for any other modern business). Rather, Authenticom alleges that its behavior creates no cybersecurity risk and that defendants are using cybersecurity as a "pretext." Compl. ¶ 236. But that allegation holds no water, for several reasons.

For one thing, Authenticom has not plausibly alleged that its own behavior creates no cybersecurity risk to defendants' systems. It alleges that it has "never had a data breach" (Compl. ¶ 240)—but even if true, that is hardly a guarantee that one would not occur in the future. It also touts its use of "standard industry protocols" and its purported "gold security certification" from Microsoft, but it provides no details about these subjects. *Id.* And although Authenticom alleges it has a "$20 million dollar cyber liability insurance policy" (*id.*), it offers no allegations sufficient to establish that this is adequate insurance against losses from a cyber attack. In any event, CDK's access policies applied not just to Authenticom, but also to all other "integrators" and third parties, many of which may have had different security measures. Thus, even it Authenticom *itself* were not a security risk, that would not show that CDK's concern for cybersecurity was pretextual.

Authenticom's other "pretext" arguments are likewise meritless on their faces. It alleges that CDK permitted hostile integration on its system at one point (Compl. ¶ 237)—but again, even if true, that does not show that CDK's current concern for security is pretextual. It is commonplace for companies to alter their business practices over time in response to changed conditions. *Cf., e.g.*, *Sound of Music Co. v. Minnesota Mining & Mfg., Co.*, 389 F. Supp. 2d 988, 1008 (N.D. Ill. 2005) (noting that the "strategy of preemptively shutting down a currently profitable business because its competitive position eventually will erode over time is not illogical nor uncommon"). Authenticom also argues that its data extraction is comparable to the "screen scraping" done by data "integrators" for banking or healthcare applications (*id.* ¶ 238), but it offers no facts supporting that assertion—or supporting its claim that the data in banking and healthcare systems is "much more sensitive than anything accessible from dealers" (*id.*). Nor does Authenticom provide any facts supporting its insinuation that banks do not mind data extraction. Indeed, the Consumer Financial Protection Bureau regulation that Authenticom cites (Compl. ¶ 238 & n.38) in support of so-called "screen-scraping" also notes that "consumer financial account providers have raised concerns about whether account aggregators or permissioned parties [*i.e.*, data "integrators"] employ adequate security and privacy procedures with respect to consumers' online account credentials and consumer account data obtained through aggregation." *Request for Information Regarding Consumer Access to Financial Records*, Bureau of Consumer Fin. Protection, Dkt. No. CFPB-2016-0048, at 12-13 (Nov. 14, 2016), perma.cc/F28M-5TZU.[6]

Defendants unquestionably "had the right to [design or] redesign [their] products to make them more attractive to buyers" through "improved performance." *Allied Orthopedic*, 592 F.3d at 999 (quoting *Cal. Comput. Prods.*, 613 F.2d at 744). The antitrust laws do not impose a duty to limit "product development so as to facilitate sales of [third-party] products." *Id.* (quoting same). CDK is,

[6] As a public document prepared by a government agency, and as a document quoted in the complaint, this document is subject to judicial notice on a motion to dismiss. *See, e.g.*, *Wigod v. Wells Fargo Bank, N.A.*, 673 F.3d 547, 556 (7th Cir. 2012).

in other words, "under no duty to help [Authenticom] or other [third-party data "integrators"] survive or expand." *Id*. (quoting same). *See also Novell, Inc. v. Microsoft Corp.*, 731 F.3d 1064, 1075 (10th Cir. 2013) (Gorsuch, J.) (explaining that a dominant firm may "withdraw from a prior course of dealing . . . in order to pursue perfectly procompetitive ends—say, to pursue an innovative replacement product of its own"). That principle mandates rejection of Authenticom's claims.

II. AUTHENTICOM HAS FAILED TO STATE A CLAIM UNDER SECTION 2

"The offense of monopoly under § 2 of the Sherman Act has two elements: (1) the possession of monopoly power in the relevant market and (2) the willful acquisition or maintenance of that power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident." *United States v. Grinnell Corp.*, 384 U.S. 563, 570-71 (1966). Authenticom has failed to allege a claim under this framework. It has not plausibly alleged that CDK has monopoly power in any market, because it has not plausibly alleged that a single-brand aftermarket for data extraction on CDK's DMS exists. And even if it had plausibly alleged the existence of that single-brand market, it has not plausibly alleged that CDK's conduct was intended "to foreclose competition, to gain a competitive advantage, or to destroy a competitor." *United States v. Griffith*, 334 U.S. 100, 107 (1948).

A. There are no brand-specific aftermarkets for "data integration services"

In order to prevail on a Section 2 theory, Authenticom must demonstrate that defendants have monopoly power in a relevant market. Monopoly power "requires . . . something greater than market power" (*Eastman Kodak*, 504 U.S. at 481); such power exists only where a firm has the "ability to charge a price above the competitive level." *Sheridan v. Marathon Petroleum Co.*, 530 F.3d 590, 594 (7th Cir. 2008). Authenticom alleges that defendants have monopolized brand-specific "Dealer Data Integration aftermarkets" for their respective, brand-specific DMSs. Compl. ¶ 271. That claim cannot succeed, because these purported markets do not exist under *Kodak* or any other antitrust precedent.

Plaintiff's claim fails under *Kodak* because CDK has all along had express contract terms in place prohibiting dealers from permitting third-party access to the DMS by disseminating login credentials. *See supra* at 4-5. Dealers therefore had the opportunity, when contracting for DMS service, to choose whether or not to use a DMS that permitted hostile data extraction, and to weigh the potential lifecycle costs of each approach. That precludes any claim that dealers are unfairly "locked in" to CDK's DMS within the meaning of *Kodak*—as the Seventh Circuit has explained, if a seller "informed customers about its policies before they bought," "purchasers could have shopped around" and thus cannot have been unfairly locked in. *Dig. Equip. Corp. v. Uniq Dig. Techs., Inc.*, 73 F.3d 756, 763 (7th Cir. 1996). On this point, there is no room for debate: If a secondary product or service is "bundled" with a secondary service or product "from the outset," it follows that "purchasers could have shopped around for competitive life-cycle prices" all along and are not unfairly locked in. *Id.*; *see also, e.g., DSM Desotech Inc. v. 3D Sys. Corp.*, 749 F.3d 1332, 1346 (Fed. Cir. 2014) ("Crucial to the *Kodak* decision . . . was the fact that customers had already purchased their equipment before learning about Kodak's policies on aftermarket parts and services."); *PSI Repair Servs., Inc. v. Honeywell, Inc.*, 104 F.3d 811, 820 (6th Cir. 1997) ("[T]he change in policy in *Kodak* was the crucial factor in the Court's decision. By changing its policy after its customers were 'locked in,' Kodak took advantage of the fact that its customers lacked the information to anticipate this change.").

Authenticom may argue that, prior to 2015, CDK is alleged not to have enforced the contractual bars on third-party access to its DMS platform—but that is no help to Authenticom. The express prohibition on unauthorized access to CDK's DMS platforms (which is to say, the express prohibition on hostile, third-party data extraction) was a term of CDK's contracts with its dealers. Even if they believed there was a chance that CDK might not enforce those terms, they would have been aware of the term and the possibility that the provision *would* be enforced. "A party is not justified in relying on representations outside of or contrary to the written terms of a contract he or

she signs when the signer is aware of the nature of the contract and had a full opportunity to read it." *See Cromeens, Holloman, Sibert, Inc. v. AB Volvo*, 349 F.3d 376, 394 (7th Cir. 2003).

Thus, even if there were a brand-specific aftermarket for data "integration" on CDK's DMS, Authenticom could not complain about CDK's market power in that market because dealers voluntarily agree to restrictions on third-party access to that DMS. As a number of courts have held, "the law prohibits an antitrust [plaintiff] from resting on market power [in an aftermarket] that arises solely from contractual rights that consumers knowingly and voluntarily gave to the defendant." *Newcal Indus., Inc. v. Ikon Office Sol.*, 513 F.3d 1038, 1048 (9th Cir. 2008) (emphasis omitted). The reason why is clear: When a primary market is competitive and restrictions on any aftermarkets are contractually agreed to by consumers in the primary market, competition in the primary market will necessarily discipline the aftermarkets. *See, e.g.*, *Queen City Pizza, Inc. v. Domino's Pizza, Inc.*, 124 F.3d 430, 441 (3d Cir. 1997). That principle is controlling here. Because dealers all along have freely agreed that they will not give unauthorized access to the DMS to third parties like Authenticom, the enforcement of such contractual restrictions does not offend the antitrust laws.

That is all the more true in this case because CDK's decision to prohibit third-party access to its DMS renders Authenticom's business model unlawful under the Computer Fraud and Abuse Act ("CFAA"), which imposes criminal liability on anyone who "[1] intentionally accesses a computer without authorization or exceeds authorized access, and [2] thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2); *see, e.g.*, *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1067-68 (9th Cir. 2016) (defendant's unauthorized access of plaintiff's computers to aggregate users' data violated CFAA), *petition for cert. filed*, No. 16-1105; *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 581 (1st Cir. 2001) (defendants' unauthorized access of website to obtain information through "scraper" violated CFAA); *Craigslist Inc. v. 3Taps Inc.*, 964 F. Supp. 2d 1178, 1187 (N.D. Cal. 2013) (same). Authenticom cannot complain about the alleged foreclosure of competition in a market for services that not only violate contractual terms its customers voluntarily

accepted, but that are (as a consequence) illegal under federal law. *See Modesto Irrigation Dist. v. Pac. Gas & Elec. Co.*, 309 F. Supp. 2d 1156, 1169-70 (N.D. Cal. 2004) ("Courts have long recognized that 'an action under the antitrust laws will not lie where the business conducted by the plaintiff, and alleged to have been restrained by the defendant, was itself unlawful.").

In sum, if dealers wish to use a DMS provider that permits unchecked third-party data extraction and want to assume all of the risks that come along with it, they are free to do business with a different DMS provider. The fact that many of CDK's customers decide *not* to switch (Compl. ¶ 42) is not an indication that they are "locked in" to defendants' systems.

B. CDK has no duty under the antitrust laws to ignore the plain terms of its service agreements and permit hostile data "integrators" to access its DMS

Authenticom also fails to establish predatory conduct sufficient to support its Section 2 claim. On this score, Authenticom asserts that it was "exclusionary" for CDK to refuse to allow hostile data "integrators" like Authenticom to gain access to its secure, proprietary DMS platform for free. But as we have explained, the closure of CDK's DMS platform to third-party data "integrators" is a necessary element of its procompetitive SecurityFirst program. Again, CDK "had the right to [design and] redesign its products to make them more attractive to buyers" through "improved performance," and the antitrust laws do not impose a duty on it to limit "product development so as to facilitate sales of [Authenticom's] products." *Allied Orthopedic*, 592 F.3d at 999 (quoting *Cal. Comput. Prods., Inc.*, 613 F.2d at 744).

More fundamentally, "the Sherman Act 'does not restrict the long recognized right of [a] trader or manufacturer engaged in an entirely private business, freely to exercise his own independent discretion as to parties with whom he will deal.'" *Verizon Commc'ns Inc. v. Law Offices of Curtis V. Trinko, LLP*, 540 U.S. 398, 408 (2004) (quoting *United States v. Colgate & Co.*, 250 U.S. 300, 307 (1919)); *accord, e.g., Pac. Bell Tel. Co. v. Linkline Commc'ns, Inc.*, 555 U.S. 438, 448 (2009) ("As a general rule, businesses are free to choose the parties with whom they will deal, as

well as the prices, terms, and conditions of that dealing."). That rule, as the Seventh Circuit has explained, is based on the simple premise that "[c]ooperation is a problem in antitrust, not one of its obligations." *Schor v. Abbott Labs.*, 457 F.3d 608, 610 (7th Cir. 2006) (emphasis omitted). Thus, "antitrust law does not require monopolists to cooperate with rivals" or any other third parties. *Id.*

To be sure, the right to refrain from aiding other businesses is not "unqualified." *See Aspen Skiing*, 472 U.S. at 601. But courts have been "very cautious in recognizing" exceptions to this right, "because of the uncertain virtue of forced sharing and the difficulty of identifying and remedying anticompetitive conduct by a single firm." *Trinko*, 540 U.S. at 408. For example, in *Aspen Skiing*, the Court recognized that a refusal to deal was anticompetitive if the defendant's behavior was economically irrational absent a desire to monopolize, in that the defendant sacrificed short-term gain (sales at its own retail price) in order to destroy a rival. 472 U.S. at 608. But this example, the Court later explained, "is at or near the outer boundary of § 2 liability." *Trinko*, 540 U.S. at 409. In general, where a refusal to deal has any rational business justification, the courts will not declare the refusal to be a violation of the antitrust laws. *See* Areeda & Hovenkamp ¶ 772c2 ("*Aspen* leaves monopolists free to refuse to deal or cooperate with rivals for legitimate business reasons.").

That principle alone disposes of Authenticom's Section 2 claim. Authenticom complains that CDK declined to give it access to its DMS platform—but CDK had no duty to give that access in the first place. CDK's dealer management system is a proprietary platform that has been developed through enormous investments of time and resources, *and its service contracts with dealers expressly forbid the kind of access that Authenticom seeks*. CDK is under no obligation to disregard the clear terms of its service contracts to help Authenticom and others do business. After all, "[t]he antitrust laws protect consumers, not producers." *Sanderson v. Culligan Int'l Co.*, 415 F.3d 620, 623 (7th Cir. 2005). For its part, Authenticom wants to offer its own data extraction service that parasitizes CDK's considerable investments in the creation and maintenance of its DMS platform.

Section 2 does not require CDK to reorder its own business practices to prop up Authenticom's free-riding business model, and Authenticom's Section 2 claim therefore fails as a matter of law.

III. AUTHENTICOM HAS FAILED TO STATE A CLAIM FOR TORTIOUS INTERFERENCE WITH CONTRACT

Finally, Authenticom has failed to state a claim for tortious interference with contract. In Wisconsin, tortious interference "requires proof of the following five elements: '(1) the plaintiff had a contract or prospective contractual relationship with a third party; (2) the defendant interfered with the relationship; (3) the interference was intentional; (4) a causal connection exists between the interference and the damages; and (5) the defendant was not justified or privileged to interfere.'" *Comsys Inc. v. City of Kenosha*, 2017 WL 1906750, at *22 (E.D. Wis. May 9, 2017) (quoting *Burbank Grease Servs., LLC v. Sokolowski*, 294 Wis. 2d 274, 304, 717 N.W.2d 781, 796 (2006)). Authenticom has not plausibly alleged that these elements are satisfied here. Even assuming that CDK's decision not to permit Authenticom to access its DMS directly rose to the level of "interference" with Authenticom's vendor contracts (in fact, the inverse is true), the decision was made to protect CDK's *own* contractual rights.

The Restatement creates an exception to tortious-interference liability where, as here, the defendants act to vindicate their own contractual rights. Simply put, "[o]ne who, by asserting in good faith a legally protected interest of his own . . . intentionally causes a third person not to perform an existing contract . . . does not interfere improperly with the other's relation if the actor believes that his [or her] interest may otherwise be impaired or destroyed by the performance of the contract or transaction." Restatement (Second) of Torts § 773 (Am. Law Inst. 1979).[7] *Accord, e.g., Thompson Everett, Inc. v. Nat'l Cable Advert., L.P.*, 850 F. Supp. 470, 482 (E.D. Va. 1994) (no tortious-interference liability where "defendants acted in good faith to protect their [own] contractual

[7] Wisconsin courts follow the Restatement (Second) of Torts' approach to the tortious-interference cause of action. *See Magnum Radio, Inc. v. Brieske*, 217 Wis. 2d 130, 136, 577 N.W.2d 377, 379 (Ct. App. 1998); *Cudd v. Crownhart*, 122 Wis. 2d 656, 660, 364 N.W.2d 158, 161 (Ct. App. 1985).

rights"), *aff'd*, 57 F.3d 1317 (4th Cir. 1995); *Briesemeister v. Lehner*, 2006 WI App 140, ¶ 54, 295 Wis. 2d 429, 455, 720 N.W.2d 531, 544 (Ct. App.) ("A party has a right to protect what he believes to be his legal interest."); *id.* ¶ 52 (citing Restatement (Second) of Torts § 773); *Cudd*, 122 Wis. 2d at 662, 364 N.W.2d at 161 ("As the Restatement makes clear, a party has a right to protect what he believes to be his legal interest.") .

That exception undoubtedly applies here. CDK's contracts with dealers permit CDK to deny any third-party access to the DMS. Compl. ¶ 151. By purportedly "blocking" Authenticom, therefore, CDK did no more than stand on its own contractual rights in order to prevent harm to its businesses and to its customers' data. Under prevailing law, that decision was not tortious interference with any contract of Authenticom's.

CONCLUSION

The complaint should be dismissed.

Dated: July 21, 2017

Respectfully submitted,

/s/ *Mark W. Ryan*

MARK W. RYAN
MICHAEL B. KIMBERLY
MATTHEW A. WARING
Mayer Brown LLP
1999 K Street NW
Washington, DC 20006
(202) 263-3000

BRITT M. MILLER
MATTHEW D. PROVANCE
Mayer Brown LLP
71 S Wacker Drive
Chicago, IL 60606
(312) 782-0600

JEFFREY A. SIMMONS
JOSEPH S. HARPER
Foley & Lardner LLP
150 East Gilman Street
P.O. Box 1497
Madison, WI 53701-1497
(608) 257-5035

Counsel for Defendant
CDK Global, LLC

REDACTED VERSION

Exhibits 1-3

REDACTED

PURSUANT TO PROTECTIVE ORDER